

JAMES R. LANGEVIN
2ND DISTRICT, RHODE ISLAND

COMMITTEE ON ARMED SERVICES

EMERGING THREATS AND CAPABILITIES
(RANKING)

SEAPOW AND PROJECTION FORCES
TACTICAL AIR AND LAND FORCES

COMMITTEE ON
HOMELAND SECURITY

CYBERSECURITY AND INFRASTRUCTURE
PROTECTION

EMERGENCY PREPAREDNESS, RESPONSE,
AND COMMUNICATIONS

Congress of the United States
House of Representatives
Washington, DC 20515-3902

WASHINGTON OFFICE:
2077 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225-2735
FAX: (202) 225-5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732-9400
FAX: (401) 737-2982

<https://langevin.house.gov>

July 27, 2018

The Honorable Kirstjen M. Nielsen
Secretary of Homeland Security
Washington, DC 20528

Dear Secretary Nielsen,

I am writing in furtherance of the Department of Homeland Security's efforts to formalize a coordinated vulnerability disclosure (CVD) program as we discussed during your testimony before the House Committee on Homeland Security in April. I have long had an abiding interest in encouraging the adoption of cybersecurity best practices, and I am very interested in understanding the progress that the Department has made in developing and publishing a vulnerability disclosure policy.

With 39 major information technology (IT) investments and \$6.8B in IT spending in fiscal year 2018 alone¹, the Department must leverage every tool and partner available to secure its IT infrastructure. A vulnerability disclosure program would enhance the Department's access to the talents and resources of security testers everywhere for the purpose of securing DHS's systems. Your new cybersecurity strategy rightly emphasizes the importance of collaboration with nonfederal partners, and notes that, "[w]ithin its own systems, DHS must continue to...serve as a model for other agencies in the implementation of cybersecurity best practices."² As noted in the new version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, vulnerability disclosure programs have become an established best practice³.

Vulnerability disclosure practices are reflected in industry standards, including the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)'s information technology standards⁴ and the Center for Internet Security Controls⁵. The Carnegie Mellon University

¹ Office of Management and Budget, "Agency Summary – Department of Homeland Security | IT Dashboard," <https://itdashboard.gov/drupal/summary/024> (May 2018)

² "U.S. Department of Homeland Security Cybersecurity Strategy," https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (May 15, 2018): 5, 8

³ National Institute for Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," <https://doi.org/10.6028/NIST.CSWP.04162018> (April 16, 2018). See control RS.AN-5.

⁴ International Standards Organization/International Electrotechnical Commission Joint Technical Committee 1, "ISO/IEC 29147:2014, Vulnerability disclosure," http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip (February 15, 2014)

⁵ Center for Internet Security, "CIS Controls Version 7," <https://www.cisecurity.org/controls/> (March 19, 2018). See, for example, control 18.8.

Software Engineering Institute has published a comprehensive guide on the subject⁶. Many of your federal agency partners beyond NIST have also produced standards and guidance for vulnerability disclosure. The National Telecommunications and Information Association has partnered with the Forum of Incident Response and Security Teams to publish a collection of resources and guidelines for vulnerability coordination and disclosure⁷. The Department of Justice's Cybersecurity Unit has released a framework to assist in the formation of formal vulnerability disclosure programs⁸.

The National Cybersecurity and Communications Integration Center (NCCIC) already conducts valuable vulnerability disclosure activities as a third-party coordination center. NCCIC Industrial Control Systems (ICS) receives reports of vulnerabilities in ICS products, coordinates with affected product developers to confirm the flaws and verify mitigations, and helps disseminate information to end users in critical infrastructure sectors about the vulnerabilities and corrections available. However, beyond coordinating vulnerability disclosure with third parties, DHS must be better positioned to receive reports about first-party software flaws in its information and communications technology (ICT).

Many of my Congressional colleagues have proposed measures relating to bug bounty programs at departments and agencies. While I strongly support the inclusion of bug bounties in a robust vulnerability disclosure program when appropriate, offering financial or other remuneration for reporting a bug only works when built on the foundation of a reporting, triage, remediation, and communication framework. The reward is only one small part of the process, and, as I have learned from my time interacting with the security research community, many individuals will freely report vulnerabilities simply to make the Internet a safer place. It is also worth noting that, beyond the infrastructure needed to run a vulnerability disclosure program, whether it includes bug bounty or not, there also need to be clearly communicated guidelines governing the actions of security researchers. These are the formal elements that the Department has yet to implement with respect to ICT that it owns and operates.

During the formalization process, I encourage you to leverage the work of the Department of Defense (DoD) and the General Services Administration (GSA), both of which have implemented robust vulnerability disclosure programs. While the "Hack the Pentagon" bug bounty program that started in 2016 may be better known, DoD's vulnerability disclosure program⁹ underpins its continuing bug bounty events. GSA's published vulnerability disclosure policy¹⁰, like DoD's, clearly lays out the network domains covered by the disclosure program, the types of testing authorized, the rights of security testers, instructions for securely reporting vulnerabilities, and rules about disclosing security bugs after they have been reported.

I hope to see the Department embrace similar practices and publish a clear policy specifying DHS's treatment of vulnerability reports, instructions for discoverers to report security bugs, and information

⁶ Householder, Allen D. et al., "The CERT® Guide to Coordinated Vulnerability Disclosure," https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf (August 2017)

⁷ "Vulnerability Coordination SIG," <https://www.first.org/global/sigs/vulnerability-coordination/> (May 5, 2018)

⁸ "A Framework for a Vulnerability Disclosure Program for Online Systems," <https://www.justice.gov/criminal-ccips/page/file/983996/download> (July 2017)

⁹ "U.S. Dept Of Defense: Vulnerability Disclosure via HackerOne", <https://hackerone.com/deptofdefense> (November 21, 2016)

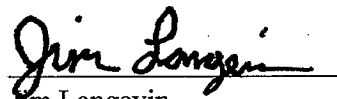
¹⁰ General Services Administration, "18F: Digital service delivery | Vulnerability disclosure policy," <https://18f.gsa.gov/vulnerability-disclosure-policy/> (March 26, 2018)

about how the Department will address and disclose such reports. Such a policy, in concert with reporting instructions, a commitment by the Department to make triage decisions about reported vulnerabilities and communicate them, and outreach to security researchers and testers will help DHS tap into a large pool of talent for securing DHS's systems. Even without a bug bounty program, skilled bug hunters can serve as a "force multiplier" in the race to stay ahead of the evolving cyber threat.

As I stated during the April hearing, I remain committed to working with you to formalize a coordinated vulnerability disclosure program for DHS. If there are any barriers preventing its establishment, I trust you will promptly inform me and my staff. I would also appreciate an update on the timeline you envision for formalization.

Thank you for your continued attention to DHS's leadership in cybersecurity. Please do not hesitate to contact me or Nick Leiserson on my staff if you have any questions regarding this request, and I look forward to hearing more about your progress in standing up a vulnerability disclosure program.

Sincerely,

A handwritten signature in black ink, reading "Jim Langevin", written over a horizontal line.

Jim Langevin
Member of Congress

CC: The Honorable Christopher J. Krebs